RESEARCH CENTRE

Grenoble - Rhône-Alpes

2020
ACTIVITY REPORT

Project-Team

PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

IN COLLABORATION WITH: Centre of Innovation in Telecommunications and Integration of services

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Contents

Project-Team PRIVATICS

Creation of the Team: 2013 January 01, updated into Project-Team: 2014 July 01

Keywords

Computer sciences and digital sciences

A1.2.5. – Internet of things

A1.2.6. – Sensor networks

A1.3.1. – Web

A2.1.11. – Proof languages

A4. – Security and privacy

A4.2. – Correcting codes

A4.8. – Privacy-enhancing technologies

A9.2. – Machine learning

Other research topics and application domains

B2.3. – Epidemiology

B2.7.2. – Health monitoring systems

B6. – IT and telecom

B6.2.2. – Radio technology

B6.3.1. – Web

B6.3.2. – Network protocols

B6.3.4. – Social Networks

B6.4. – Internet of things

B6.6. – Embedded systems

B7.2. – Smart travel

B7.2.1. – Smart vehicles

B7.2.2. – Smart road

B8.1.2. – Sensor networks for smart buildings

B8.2. – Connected city

B8.5. – Smart society

B9.1.1. – E-learning, MOOC

B9.5.6. – Data science

B9.6.1. – Psychology

B9.6.2. – Juridical science

B9.9. – Ethics

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Vincent Roca [Team leader, Inria, Researcher, HDR]
- Nataliia Bielova [Inria, Researcher, from Apr 2020]
- Claude Castelluccia [Inria, Senior Researcher, HDR]
- Cédric Lauradoux [Inria, Researcher]
- Daniel Le Metayer [Inria, Senior Researcher, HDR]

Faculty Members

- Antoine Boutet [INSA Lyon, Associate Professor]
- Mathieu Cunche [INSA Lyon, Associate Professor]

Post-Doctoral Fellow

- Ruba Ali Mahmoud Abu-Salma [Inria, from Apr 2020 until Jul 2020]

PhD Students

- Supriya Sreekant Adhatarao [Inria]
- Coline Boniface [Univ Grenoble Alpes]
- Guillaume Celosia [INSA Lyon, until Oct 2020]
- Imane Fouad [Inria, from Apr 2020]
- Clement Henin [Ministère de l'Ecologie, de l'Energie, du Développement durable et de la Mer]
- Theo Jourdan [INSERM]
- Raouf Kerkouche [Univ Grenoble Alpes]
- Suzanne Lansade [Inria, from Oct 2020]
- Mathieu Thiery [Inria, until Jul 2020]
- Michael Toth [Inria, from Oct 2019]

Technical Staff

- Adrien Baud [Inria, Engineer]

Interns and Apprentices

- Jan Aalmoes [Univ Claude Bernard, from May 2020 until Jul 2020]
- Remi Coudert [École polytechnique fédérale de Lausanne, from Feb 2020 until Jul 2020]
- Hugo Degeorges [INSA Lyon, from Jun 2020 until Aug 2020]
- Remi Depreux [Institut polytechnique de Grenoble, from Feb 2020 until Jul 2020]
- Guillaume Kessibi [Institut polytechnique de Grenoble, from Feb 2020 until Jul 2020]
- Suzanne Lansade [Univ de Bordeaux, from Mar 2020 until Aug 2020]

- Lucas Toulier Ancian [INSA Lyon, from Feb 2020 until Jul 2020]
- Vera Wesselkamp [Université technique de Brunswick - Allemagne, from Sep 2020]

Administrative Assistant

- Helen Pouchot-Rouge-Blanc [Inria]

External Collaborators

- Victor Morel [Univ Grenoble Alpes, until Aug 2020]
- Cristiana Santos [School of Law, Utrecht University, From 2020, HDR]

2 Overall objectives

2.1 Context

Since its creation in 2014, the PRIVATICS project-team focusses on privacy protection in the digital world. It includes, on one side, activities that aim at understanding the domain and its evolution, both from theoretical and practical aspects, and, on the other side, activities that aim at designing privacy-enhancing tools and systems. The approach taken in PRIVATICS is fundamentally inter-disciplinary and covers theoretical, legal, economical, sociological and ethical aspects by the means of enriched collaborations with the members of these disciplines.

3 Research program

4 Application domains

4.1 Domain 1: Privacy in smart environments

One illustrative example is our latest work on privacy-preserving smart-metering [2]. Several countries throughout the world are planning to deploy smart meters in house-holds in the very near future. Traditional electrical meters only measure total consumption on a given period of time (i.e., one month or one year). As such, they do not provide accurate information of when the energy was consumed. Smart meters, instead, monitor and report consumption in intervals of few minutes. They allow the utility provider to monitor, almost in real-time, consumption and possibly adjust generation and prices according to the demand. Billing customers by how much is consumed and at what time of day will probably change consumption habits to help matching energy consumption with production. In the longer term, with the advent of smart appliances, it is expected that the smart grid will remotely control selected appliances to reduce demand. Although smart metering might help improving energy management, it creates many new privacy problems. Smart-meters provide very accurate consumption data to electricity providers. As the interval of data collected by smart meters decreases, the ability to disaggregate low-resolution data increases. Analysing high-resolution consumption data, Non-intrusive Appliance Load Monitoring (NALM) can be used to identify a remarkable number of electric appliances (e.g., water heaters, well pumps, furnace blowers, refrigerators, and air conditioners) employing exhaustive appliance signature libraries. We developed DREAM, DiffeRentially privatE smArt Metering, a scheme that is private under the differential privacy model and therefore provides strong and provable guarantees. With our scheme, an (electricity) supplier can periodically collect data from smart-meters and derive aggregated statistics while learning only limited information about the activities of individual households. For example, a supplier cannot tell from a user's trace when he watched TV or turned on heating.

4.2 Domain 2: Big Data and Privacy

We believe that another important problem will be related to privacy issues in big data. Public datasets are used in a variety of applications spanning from genome and web usage analysis to location-based and recommendation systems. Publishing such datasets is important since they can help us analyzing and understanding interesting patterns. For example, mobility trajectories have become widely collected in recent years and have opened the possibility to improve our understanding of large-scale social networks by investigating how people exchange information, interact, and develop social interactions. With billions of handsets in use worldwide, the quantity of mobility data is gigantic. When aggregated, they can help understand complex processes, such as the spread of viruses, and build better transportation systems. While the benefits provided by these datasets are indisputable, they unfortunately pose a considerable threat to individual privacy. In fact, mobility trajectories might be used by a malicious attacker to discover potential sensitive information about a user, such as his habits, religion or relationships. Because privacy is so important to people, companies and researchers are reluctant to publish datasets by fear of being held responsible for potential privacy breaches. As a result, only very few of them are actually released and available. This limits our ability to analyze such data to derive information that could benefit the general public. It is now an urgent need to develop Privacy-Preserving Data Analytics (PPDA) systems that collect and transform raw data into a version that is immunized against privacy attacks but that still preserves useful information for data analysis. This is one of the objectives of Privatics. There exists two classes of PPDA according to whether the entity that is collecting and anonymizing the data is trusted or not. In the trusted model, that we refer to as Privacy-Preserving Data Publishing (PPDP), individuals trust the publisher to which they disclose their data. In the untrusted model, that we refer to as Privacy-Preserving Data Collection (PPDC), individuals do not trust the data publisher. They may add some noise to their data to protect sensitive information from the data publisher.

Privacy-Preserving Data Publishing: In the trusted model, individuals trust the data publisher and disclose all their data to it. For example, in a medical scenario, patients give their true information to hospitals to receive proper treatment. It is then the responsibility of the data publisher to protect privacy of the individuals' personal data. To prevent potential data leakage, datasets must be sanitized before possible release. Several proposals have been recently proposed to release private data under the Differential Privacy model [25, 56, 26, 57, 50]. However most of these schemes release a "snapshot" of the datasets at a given period of time. This release often consists of histograms. They can, for example, show the distributions of some pathologies (such as cancer, flu, HIV, hepatitis, etc.) in a given population. For many analytics applications, "snapshots" of data are not enough, and sequential data are required. Furthermore, current work focusses on rather simple data structures, such as numerical data. Release of more complex data, such as graphs, are often also very useful. For example, recommendation systems need the sequences of visited websites or bought items. They also need to analyse people connection graphs to identify the best products to recommend. Network trace analytics also rely on sequences of events to detect anomalies or intrusions. Similarly, traffic analytics applications typically need sequences of visited places of each user. In fact, it is often essential for these applications to know that user A moved from position 1 to position 2, or at least to learn the probability of a move from position 1 to position 2. Histograms would typically represent the number of users in position 1 and position 2, but would not provide the number of users that moved from position 1 to position 2. Due to the inherent sequentiality and high-dimensionality of sequential data, one major challenge of applying current data sanitization solutions on sequential data comes from the uniqueness of sequences (e.g., very few sequences are identical). This fact makes existing techniques result in poor utility. Schemes to privately release data with complex data structures, such as sequential, relational and graph data, are required. This is one the goals of Privatics. In our current work, we address this challenge by employing a variable-length n-gram model, which extracts the essential information of a sequential database in terms of a set of variable-length n - grams [15]. We then intend to extend this approach to more complex data structures.

Privacy-Preserving Data Collection: In the untrusted model, individuals do not trust their data publisher. For example, websites commonly use third party web analytics services, such as Google Analytics to obtain aggregate traffic statistics such as most visited pages, visitors' countries, etc. Similarly, other applications, such as smart metering or targeted advertising applications, are also tracking users in order to derive aggregated information about a particular class of users. Unfortunately, to obtain this aggregate information, services need to track users, resulting in a violation of user privacy. One of our goals is to develop Privacy-Preserving Data Collection solutions. We propose to study whether it is possible to provide efficient collection/aggregation solutions without tracking users, i.e. without getting or learning individual contributions.

5 Social and environmental responsibility

5.1 Environmental impacts of research results

The activities of PRIVATICS are not directly related to environmental considerations. However, promoting privacy in a connected world sometimes leads us to promote local data processing, as opposed to massive data collection and big data (e.g., in the case of Internet of Things systems). From this point of view, we believe that our research results are fully aligned with environmental considerations.

5.2 Societal impacts of research results

Several of PRIVATICS works had major societal impacts. One can cite:

- The ROBERT Exposure Notification Protocol that is the foundation of the StopCovid/TousAntiCovid application;
- The work on tracking technologies and the use of consent banners in web browsers. This work helped revealing practices in the field, sometimes highlighting illegal practices, and therefore it helped promoting a more privacy friendly society;
- MOOC: Cédric Lauradoux, Nataliia Bielova and Vincent Roca *"Protection de la vie privée dans le monde numérique"* on FUN-MOOC;

6 Highlights of the year

6.1 The ROBERT Exposure Notification Protocol and the StopCovid/TousAntiCovid Application

On April, PRIVATICS proposed a "centralized" approach that later became the foundation of the StopCovid / TousAntiCovid application.

Nine months after its launch (June 2^{nd} 2020), the TousAntiCovid application has been downloaded and installed by more than 13 Million users, 180 000 users uploaded their contact proximity, and more than 100 000 users have received an "at risk" notification (mid-March 2021). Besides, the TousAntiCovid app has become a key central component of the French health strategy in the COVID-19 fight, being a multi-service application at the service of the French citizen.

More information: see section "New Results"

7 New software and platforms

7.1 New software

7.1.1 Wombat

Name: Wi-Fi tracking system for testing and demonstrational purpose

Keywords: Wi-Fi, Privacy, Multimodal tracking of human activity, Wireless network

Functional Description: Wombat is a fully functional Wi-Fi tracking platform supporting three main features: collection, storage/processing, query/output. These three features are implemented through a distributed infrastructure composed of:

Sensor nodes: small devices with wireless monitoring capabilities. They collect information sent on wireless channels and forward it to the server. Central server: the central entity of the system.

It receives data sent by sensor nodes and then stores it in an internal data structure. It is also in charge of answering queries related to the stored data.

To ensure communication between the sensor nodes and the server, the Wombat system relies on a wired network (Ethernet). In addition, Wombat can be enriched with a user interface and an opt-out node:

User interface: a device in charge of displaying detailed information about one or several tracked devices (see figure below). The device to display can be specified manually by its MAC address or through proximity detection. Opt-out node: an element in charge of implementing an opt-out mechanism for users refusing to be tracked by the system.

The system is made to work on a dedicated network (the server includes a DHCP server). Nodes can be switched off at any time (they function in read-only mode to be crash-proof).

URL: https://github.com/Perdu/wombat

Contact: Mathieu Cunche

Partner: Insa de Lyon

7.1.2 Cookie glasses

Keywords: GDPR, Cookie, Consent

Scientific Description: In the paper Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, we show that Consent Management Providers (CMPs) of IAB Europe's Transparency & Consent Framework (TCF) do not always respect user's choice. This extension allows users to verify that their consent is stored appropriately by themselves.

This extension for Firefox and Chrome queries CMPs of IAB Europe's TCF in the same position as a third-party advertiser, making it possible to see consent set by CMPs in real time. In other words, you can see whether consent registered by cookie banners is actually the consent you gave. Will only work with cookie banners of IAB Europe's TCF.

We also added a functionality to manually decode a so-called "consent string" of the framework.

Functional Description: In the paper Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, we show that Consent Management Providers (CMPs) of IAB Europe's Transparency & Consent Framework (TCF) do not always respect user's choice. This extension allows users to verify that their consent is stored appropriately by themselves.

This extension for Firefox and Chrome queries CMPs of IAB Europe's TCF in the same position as a third-party advertiser, making it possible to see consent set by CMPs in real time. In other words, you can see whether consent registered by cookie banners is actually the consent you gave. Will only work with cookie banners of IAB Europe's TCF.

We also added a functionality to manually decode a so-called "consent string" of the framework.

Contact: Alain Prette

Participants: Célestin Matte, Nataliia Bielova

7.1.3 DÉSIRÉ

Name: DÉSIRÉ: a third way for a European exposure notification system

Keywords: COVID-19, Contact tracing

Functional Description: On April 2020, the PRIVATICS Inria team (FR) and the Fraunhofer (DE) colleagues designed the CNIL-approved ROBERT privacy preserving exposure notification protocol, used by the French StopCovid/TousAntiCovid national app, and available since June 2nd. The PRIVATICS team also designed the DESIRE protocol on May 2020, as an advanced solution.

The present software is a Proof of Concept of the DÉSIRÉ protocol for Android smartphones.

Publication: https://hal.inria.fr/hal-02570382

Contact: Antoine Boutet

Participants: Adrien Baud, Pierre-Guillaume Raverdy, Christophe Braillon, Antoine Boutet, Mathieu Cunche, Vincent Roca, Claude Castelluccia

7.1.4 Cookinspect

Keywords: GDPR, Consent, Measures, Web

Functional Description: In the paper "Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework", we show that Consent Management Providers (CMPs) of IAB Europe's Transparency & Consent Framework (TCF) do not always respect user's choice. Cookinspect is a crawler that allows users to detect violations related to consent stored by the CMPs.

URL: `https://github.com/Perdu/Cookinspect`

Contact: Alain Prette

Participants: Nataliia Bielova, Célestin Matte

8 New results

8.1 The ROBERT Exposure Notification Protocol and the StopCovid/TousAntiCovid Application

Participants: Nataliia Bielova, Antoie Boutet, Claude Castelluccia, Mathieu Cunche, Cedric Lauradoux, Daniel Le Metayer, Vincent Roca.

On April, PRIVATICS proposed a "centralized" approach that later became the foundation of the StopCovid / TousAntiCovid application. More precisely:

- risk analysis is carried in a central server that necessarily keeps some information (e.g., pseudonyms of users potentially at risk);
- under the control of the Health Authority, the data controller;
- the system is continuously audited by the CNIL French Data Protection Agency.

We followed several key goals with ROBERT:

- (Goal 1) be efficient: it's of course the primary goal of any exposure notification app;
- (Goal 2) be sovereign: because this is the only way to keep full control of technical choices and citizen's data;
- (Goal 3) be privacy friendly: such a service is sensitive, and privacy - our research topic - is a must.

Being centralized is clearly a plus from an epidemiological viewpoint (real-time monitoring, real-time adjustment to conditions, better statistics), compared to a decentralized scheme like GAEN. This is in line with our Efficiency (Goal 1) and it remains the primary goal of any exposure notification system.

Being sovereign (Goal 2) is the only reasonable approach to keep control of citizen's health data, in a context where Alphabet enters the health insurance business. Being sovereign is also the only reasonable approach to keep control of the technology and minimize dependency on Google and Apple. For instance, CNIL insisted on May that the use of Google Re-Captcha service be removed, which has been done with StopCovid v1.1 en of June.

Being privacy friendly (Goal 3) is no option, and one of the lessons learned is the necessity to ask our CNIL Data Protection Agency as soon as possible. We did it for ROBERT specifications (April CNIL report), the App development (May CNIL report), and now for operational deployment (September CNIL report, and now every 3 months). Thanks to that, we can say ROBERT/StopCovid is GDRP compliant.

Nine months after its launch, on June 2^{nd} 2020, mid-March 2021 the TousAntiCovid application has been downloaded and installed by more than 13 Million users, 180 000 users uploaded their contact proximity, and more than 100 000 users have received an "at risk" notification. Besides, the TousAntiCovid app has become a key central component of the French health strategy in the COVID-19 fight, being a multi-service application at the service of the French citizen.

More information:
https://privatics.inrialpes.fr/desire/
https://github.com/ROBERT-proximity-tracing/documents/

8.2 The DÉSIRÉ Exposure Notification Protocol

Participants: Nataliia Bielova, Antoie Boutet, Claude Castelluccia, Mathieu Cunche, Cedric Lauradoux, Daniel Le Metayer, Vincent Roca.

Compared to ROBERT, the DÉSIRÉ protocol relies on a radical paradigm shift: rather than using *public device* pseudonyms, it relies on *private encounter* pseudonyms, a 32-byte value that we call PET, for Private Encounter Token. A PET changes across time (every 15 min.) and devices, and is computed in a private manner by the users who met, and only them (e.g., Alice and Bob in the figure), using well-known, robust, Diffie-Hellman crypto.

This paradigm shift changes the situation quite a lot from the security and privacy viewpoints: an eavesdropper who passively listens to Bluetooth (more precisely BLE) traffic is left powerless, because he cannot compute the PET between Alice and Bob, and he'll never be in position to know that a given PET refers to this Alice/Bob encounter that day at that precise time, or to any other encounter, or even that this is a valid PET rather than a random value. A PET is secure by design! (note that in practice two 32-byte PETs are generated per encounter to avoid linkability.

Another benefit of DÉSIRÉ is that it enables either a centralized (like ROBERT), or decentralized (like GAEN) risk evaluation, or something in-between. And this architectural choice does not impact interoperability: all DÉSIRÉ deployments fully interoperate, seamlessly. It means that each country can choose what to do, in a sovereign manner. For instance:

- if citizens do trust their DPA and institutions, a centralized deployment is recommended (improved robustness in front of re-identification attacks, see GAEN section);
- if citizens don't trust their institutions and are not afraid of re-identification risks (and what it may trigger), a decentralized deployment is recommended.

This property matches our fourth design goal, be flexible (Goal 4). DÉSIRÉ is a unique solution that provides this kind of flexibility, without compromising interoperability. For this reason, we call it a "3rd way".

Thanks to the experience gained with the TousAntiCovid development, Inria engineers developed a Kotlin Android smartphone app and a Python emulated server. This work enabled to validate most protocol, cryptographic, BLE considerations, both with the centralized and decentralized modes.

More information:
https://privatics.inrialpes.fr/desire/
https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE

8.3 Quantifying Privacy Leakage in Graph Embedding

Participant: Antoine Boutet, Vasisht Duddu Graph embeddings have been proposed to map graph data to low dimensional space for downstream processing (e.g., node classification or link prediction). With the increasing collection of personal data, graph embeddings can be trained on private and sensitive data. For the first time, we quantify the privacy leakage in graph embeddings through three inference attacks targeting Graph Neural Networks. Our *membership inference attack* aims to infer whether a graph node corresponding to an individual user's data was a member of the model's private training data or not. We consider a *blackbox* setting where the adversary exploits the output prediction scores and a *whitebox* setting where the adversary has also access to the released node embeddings. Our attack provides accuracy up to 28% (blackbox) and 36% (whitebox) beyond the random guess by exploiting the distinguishable footprint between train and test data records left by the graph embedding. In our *graph reconstruction* attack, the adversary aims to reconstruct the target graph given the corresponding graph embeddings. Here, the adversary can reconstruct the graph with more than 80% of accuracy and infer the link between two nodes with ~30% more accuracy than the random guess. Finally, we propose an *attribute inference attack* where the adversary aims to infer the sensitive node attributes corresponding to an individual user. We show that the strong correlation between the graph embeddings and node attributes allows the adversary to infer sensitive information (e.g., gender or location).

8.4 Motion sensor data anonymization by time-frequency filtering

Participant: Antoine Boutet, Theo Jourdan Recent advances in wireless actimetry sensors allow recognizing human real-time activities with mobile devices. Although the analysis of data generated by these devices can have many benefits for healthcare, these data also contains private information about users without their awareness and may even cause their re-identification. In this work, we propose a privacy-preserving framework for activity recognition. The method consists of a two-step process. First, acceleration signals are encoded in the time-frequency domain by three different linear transforms. Second, we propose a method to anonymize the acceleration signals by filtering in the time-frequency domain. Finally, we evaluate our approach for the three different linear transforms with a neural network classifier by comparing the performances for activity versus identity recognition. We extensively study the validity of our framework with a reference dataset: results show an accurate activity recognition (85%) while limiting the re-identifation rate (32%). This represents a large utility improvement (19%) against a slight privacy decrease (10%) compared to state-of-the-art baseline.

8.5 Verifying Legal Compliance of Tracking technologies and Consent banners

Participants: Nataliia Bielova, Cedric Lauradoux, Cristiana Santos, Celestin Matte, Imane Fouad, Arnaud Legout, Pierre Laperdrix, Benoit Baudry, Gildas Avoine. We have set up a collaboration with a legal scholar Cristiana Santos to understand the gaps and inconsistencies between law and technology – in particular, we set up an interdisciplinary collaboration on GDPR & ePrivacy compliance for consent banners and tracking technologies.

Legal requirements for consent banners. We have studied all the requirements that the law imposes and law interpretation on consent banners and tracking technologies. This study, which took almost a year, has been published in a law international journal "Technology & Regulation" (https://techreg.org/index.php/techreg/article/view/43), and it contains 22 fine-grained legal and technical requirements to build GDPR compliant Web applications. Based on this work, we have submitted our contributions to the public consultation of the CNIL (https://hal.inria.fr/hal-02490531).

Measuring Web tracking technologies. We have proposed new methods to detect Web tracking by analyzing behavior of invisible pixels and IDs shared via browser cookies. We uncovered new collaborations between domains on 80K thousands websites and demonstrated that two popular methods to protect users from Web tracking, based on filter lists miss between 25% and 30% of the trackers that we detect (https://content.sciendo.com/view/journals/popets/2020/2/article-p499.xml). We have made an extensive survey of Browser fingerprinting [https://hal.inria.fr/hal-02864872]. This new survey has been already cited 23 times and was on a front page of HackerNews website(https://news.ycombinator.com/item?id=19838123).

Detecting GDPR & ePrivacy violations in cookie banners. We have then devised an automated analysis of consent stored behind the cookie banner interface that implement IAB Europe TCF. With this analysis, we have crawled 28K EU websites and found potential violations of the General Data Protection Regulation (GDPR) and ePrivacy directive on 54% of websites (https://hal.inria.fr/hal-03117294).

When the preliminary version of this paper was published in December 2019, "None Of Your Business" (NOYB) NGO issued 3 complaints to the French Data Protection Authority (CNIL) based on our work. NOYB used our open source “Cookie Glasses” browser extension that decodes consent stored in the browser after the user interacts with the cookie banner that relies on IAB Europe TCF. The complaint addressed three popular French websites: CDiscount, AlloCine and VanityFair.
More info: https://noyb.eu/en/say-no-cookies-yet-see-your-privacy-crumble.
Legal analysis and measurement of GDPR purpose specification principle. We have then analysed whether websites provide legally-compliant description of the purposes of their cookies (https://hal.inria.fr/hal-02567022). We have also analysed compliance of purposes that IAB Europe TCF defines for cookies banners, and how advertisers use such purposes (https://hal.inria.fr/hal-02566891). We have found that most purposes are not GDPR-compliant and their usage raises numerous questions. Based on this work, we submitted our contribution to the public consultation of the EDPB (https://hal.inria.fr/hal-03117323).

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Inria associate team not involved in an IIL

DATA Inria Associate Team

Title: *Data and Algorithmic Transparency and Accountability*

Duration: 2018 - 2021

Coordinator: Daniel Le Metayer

Partners:

- *LATECE, Université du Québec à Montréal (UQAM) (Canada)*

Inria contact: Daniel Le Metayer

Summary: The accelerated growth of the Internet has outpaced our abilities as individuals to maintain control of our personal data. The recent advent of personalized services has lead to the massive collection of personal data and the construction of detailed profiles about users. However, users have no information about the data which constitute its profile and how they are exploited by the different entities (Internet companies, telecom operators, ...). This lack of transparency gives rise to ethical issues such as discrimination or unfair processing.

In this associate team, we propose to strengthen the complementary nature and the current collaborations between the Inria Privatics group and UQAM to advance research and understanding on data and the algorithmic transparency and accountability.

9.2 European initiatives

9.2.1 FP7 & H2020 Projects

SPARTA

Title: Special projects for advanced research and technology in Europe

Duration: 2019 - 2021

Coordinator: *COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (France)*

Partners:

- CENTRE D’EXCELLENCE EN TECHNOLOGIES DE L’INFORMATION ET DE LA COMMUNICATION (Belgium)
- CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB (Czech Republic)
- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (France)
- CONSIGLIO NAZIONALE DELLE RICERCHE (Italy)
- CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L’INFORMATICA (Italy)
- CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (Italy)
- CZ.NIC, ZSPO (Czech Republic)
- DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA - ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL’INFORMAZIONE (Italy)
- FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (Germany)
- FUNDACIO EURECAT (Spain)
- FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH (Spain)
- FUNDACION TECNALIA RESEARCH INNOVATION (Spain)
- GENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA (Lithuania)
- INDRA SISTEMAS SA (Spain)
- INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS (Portugal)
- INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON (France)
- INSTITUTO SUPERIOR TECNICO (Portugal)
- ITTI SP ZOO (Poland)
- JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH (Austria)
- KAUNO TECHNOLOGIJOS UNIVERSITETAS (Lithuania)
- KENTRO MELETON ASFALEIAS
- LEONARDO - SOCIETA PER AZIONI (Italy)
- LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS (Lithuania)
- LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (Luxembourg)
- MYKOLO ROMERIO UNIVERSITETAS (Lithuania)
- NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"
- NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY (Poland)
- SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (France)
- STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO (Poland)
- TARTU ULIKOOL (Estonia)
- TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH (Austria)
- TECHNISCHE UNIVERSITAET MUENCHEN (Germany)
- THALES SIX GTS FRANCE SAS (France)
- UNIVERSITAT KONSTANZ (Germany)
- UNIVERSITE DE NAMUR ASBL (Belgium)
- UNIVERSITE DU LUXEMBOURG (Luxembourg)
- VYSOKE UCENI TECHNICKE V BRNE (Czech Republic)

Summary: SPARTA will launch and execute four Programs validating the operation of the network and performing ground-breaking advances in key areas for Europe's strategic autonomy:

- Full Spectrum Situational Awareness;
- Continuous Assessment in Polymorphous Environments;
- High-Assurance Intelligent Infrastructure Toolkit;
- Secure and Fair AI Systems for Citizen.

9.3 National initiatives

9.3.1 ANR

CISC

- Title: Certification of IoT Secure Compilation.
- Type: ANR.
- Duration: April 2018 - March 2022.
- Coordinator: Inria INDES project-team (France)
- Others partners: Inria CELTIC project-team (France), College de France (France) (France).
- See also: http://cisc.gforge.inria.fr.
- Abstract: The objective of the ANR CISC project is to investigate multitier languages and compilers to build secure IoT applications with private communication. A first goal is to extend multitier platforms by a new orchestration language that we call Hiphop.js to synchronize internal and external activities of IoT applications as a whole. CISC will define the language, semantics, attacker models, and policies for the IoT and investigate automatic implementation of privacy and security policies by multitier compilation of IoT applications. To guarantee such applications are correct, and in particular that the required security and privacy properties are achieved, the project will certify them using the Coq proof assistant.

SIDES 3.0

- Title: Application of privacy by design to biometric access control.
- Type: ANR.
- Duration: August 2017 - August 2020.
- Coordinator: Uness (France).
- Others partners: INRIA, UGA, ENS, Theia, Viseo.
- Abstract: Since 2013, faculties of medicine have used a shared national platform that enables them to carry out all of their validating exams on tablets with automatic correction. This web platform entitled SIDES allowed the preparation of the medical students to the Computerized National Classing Events (ECN) which were successfully launched in June 2016 (8000 candidates simultaneously throughout France). SIDES 3.0 proposes to upgrade the existing platform. Privatics goals in this project is to ensure that privacy is respected and correctly assessed .

DAPCODS/IOTics

- Title: DAPCODS/IOTics.
- Type: ANR 2016.
- Duration: May 2017 - Dec. 2020.
- Coordinator: Inria PRIVATICS.
- Others partners: Inria DIANA, EURECOM, Univ. Paris Sud, CNIL.
- Abstract:

  Thanks to the exponential growth of the Internet, citizens became more and more exposed to personal information leakage in their digital lives. This trend begun 20 years ago with the development of Internet. The advent of smartphones, our personal assistant always connected and equipped with many sensors, further reinforced the tendency. Today the craze for quantified-self wearable devices, smart home appliances and more generally connected devices, enable the collection of personal information – sometimes very sensitive – in domains that were so far out of reach. However, little is known about the actual practices in terms of security, confidentiality, or data exchanges. The end-user as well as the regulator are therefore prisoner of a highly asymmetric system.

  The IOTics project gathers four research teams working on security, privacy and digital economy, plus the CNIL, the French data protection agency. It focusses on connected devices and follows three directions: the analysis of the internal behavior in terms of personal information leakage of a set of connected devices; the analysis of the privacy policies provided (or not) by the device manufacturers; and the analysis of the underlying ecosystem. By giving transparent information of hidden behaviors, by highlighting good and bad practices, the IOTics project aims at reducing information asymmetry, at giving back control to the end-users and hopefully encouraging stakeholders to change practices.

PMR: Privacy-preserving methods for Medical Research

- Type: ANR
- Duration: 2020 - 2024
- Coordinator: Inria
- Others partners: Inria Magnet, Creatis
- Abstract: Given the growing awareness of privacy risks of data processing, there is an increasing interest in privacy-preserving learning. However, shortcomings in the state of the art limit the applicability of the privacy-preserving learning paradigm. First, most approaches assume too optimistically a honest-but-curious setting. Second, most approaches consider one learning task in isolation, not accounting for the context where querying is a recurring activity. In this project, we will investigate new algorithms and models that address these shortcomings. Among others, (i) our algorithms will combine privacy-preserving properties of differential privacy with security offered by cryptography and (ii) based on models of information flows in integrated data handling processes, we will build more refined models analyzing the implications of repeated querying. We will demonstrate the utility of our new theory and algorithms by proposing strategies to realistically apply them in significant real-world problems illustrated through use cases in the medical domain.

PrivaWEB: Privacy Protection and ePrivacy Compliance for Web Users

- Type: ANR JCJC
- Duration: 2018 - 2023

- Coordinator: Inria
- Abstract: PrivaWEB aims at developing new methods for detection of advanced Web tracking technologies and new tools to integrate in existing Web applications that seamlessly protect privacy of users. In this project, we will integrate three key components into Web applications: privacy, compliance and usability. Our research will address methodological aspects (designing new detection methods and privacy protection mechanisms), practical aspects (large-scale measurement of Web applications, integration in existing Web browsers), and usability aspects (user surveys to evaluate privacy concerns and usability of existing and new protection tools).

9.3.2 INRIA-CNIL collaboration

PRIVATICS is in charged of the CNIL-Inria collaboration. This collaboration was at the origin of the Mobilitics project and it is now at the source of many discussions and collaborations on data anoymisation, risk analysis, consent or IoT Privacy.

PRIVATICS and CNIL are both actively involved on the IoTics project, that is the follow-up of the Mobilitics projects. The goal of the Mobilitics project was to study information leakage in mobile phones. The goal of IoTics is to extend this work to IoT and connected devices.

PRIVATICS is also in charged of the organization of the CNIL-Inria prize that is awarded every year to an outstanding publication in the field of data privacy.

9.3.3 Inria Action de Dévelopement Technologique (ADT)

PRESERVE

- Title: PRESERVE: Plate-foRme wEb de SEnsibilisation aux pRoblèmes de Vie privéE
- Duration: 2019 - 2020
- Coordinator: INSA.
- Abstract: The goal of this project is to develop a web platform to increase the user awareness on privacy issues. This platform will gather multiple works investigated in the team and will be used to conduct demonstration and stimulate new collaborations and dissemination actions to end users and media.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

- Nataliia Bielova: *Co-president* of CNIL-Inria Privacy Protection Award 2020, Brussels, January 2020.
- Daniel Le Métayer: Computers Privacy and Data Protection (CPDP) panel *Automated facial recognition: where to put the red line ?*, Brussels, January 2020.

Member of the organizing committees

- Antoine Boutet: Winter School on Distributed Systems and Networks 2020, 3-7/02/2020, Sept Laux, France.
- Daniel Le Métayer: Co-organizer of the workshop *Intelligence artificielle, algorithmes et monde public* of the chair *Transformations de l'action publique* of Sciences-Po Lyon.
- Claude Castelluccia, *Building trust in AI, building trust with AI*, Global Science Week, 01/06/2019, Grenoble, France.

10.1.2 Scientific events: selection

Member of the conference program committees

- Cédric Lauradoux: APF 2020
- Daniel Le Métayer: APF 2020, IWPE 2020, SPOSE 2020, XAI 2020
- Nataliia Bielova: PETs 2020, TheWeb 2020, Caspar Bowden PETs Award
- Antoine Boutet: LPW 2020, DIAS 2020, APVP 2020
- Claude Castelluccia: APF 2020

10.1.3 Invited talks

- Claude Castelluccia, *A Risk Analysis Framework for Facial Recognition Applications*, Contact Tracing & Giant Data Collectors: A Journey from Utopia to Dystopia?, 01/12/2020, Online `https://tracecorona.net/events/`.
- Claude Castelluccia, *Panel on Contact Tracing*, Eurocrypt 2020, May 2020.
- Clément Henin, Daniel Le Métayer, *Explications et justifications des décisions algorithmiques*, 06/11/2020, CNIL, Online.
- Nataliia Bielova, Cristiana Santos, *Are cookie banners indeed compliant with the law?*, 03/12/2020, Cyber Security Coalition, Belgium, Online. `https://www.cybersecuritycoalition.be/webinars#gdpr`
- Nataliia Bielova, Cristiana Santos, *Are cookie banners indeed compliant with the law ?*, 12/11/2020, University Cote d'Azur, France, Online. `https://droit.univ-cotedazur.fr/dl4t/webinaires-et-podcasts-lexcast`.
- Nataliia Bielova, *Detecting online tracking and GDPR violations in Web applications*, 17/12/2020, GDR Securite, Online.
- Antoine Boutet, *DYSAN: Dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks*, 03/12/2020, ICT4V Workshop on Privacy & Anonymization, Online.
- V. Roca, *From ROBERT to DESIRE exposure notification: situation and lessons learned*, Workshop on Security and Privacy in Contact Tracing invited talk, September 2020. (YouTube record), (slides, PDF).

10.1.4 Teaching

- Master: Nataliia Bielova, *Privacy, Security and ethical aspects of Data*, 21h, Universite Cote d'Azur, France.
- Master: Nataliia Bielova, *Privacy on the Internet*, 12h, SKEMA Business School, France.
- Master : Antoine Boutet, *Privacy*, 80h, INSA-Lyon, France.
- Master : Antoine Boutet, *Security*, 40h, INSA-Lyon, France.
- Master : Antoine Boutet, *Security and Privacy*, 40h, Polytech Annecy, France.
- Master : Antoine Boutet, *Network*, 110h, INSA-Lyon, France.
- Undergraduate course : Mathieu Cunche, *Introduction to computer science*, 120h, L1, INSA-Lyon, France.
- Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

- Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.
- Undergraduate course : Mathieu Cunche, *Security & Privacy*, 21h, L3, INSA-Lyon, France.
- Master : Mathieu Cunche, *Privacy and Data protection*, 14h, M2, INSA-Lyon, France.
- Master : Mathieu Cunche, *Cryptography and Communication Security*, 18h, M1, INSA-Lyon, France.
- Master : Cédric Lauradoux, *Advanced Topics in Security*, 20h, M2, Ensimag/INPG, France.
- Master : Cédric Lauradoux, *Systems and Network Security*, 30h, M1, Ensimag, France.
- Master : Cédric Lauradoux, *Internet Security*, 12h, M2, University of Grenoble Alpes, France.
- Master : Cédric Lauradoux, *Cyber Security*, 3h, M2, Laws School of University of Grenoble Alpes, France.
- Master : Claude Castelluccia, *Advanced Topics in Security*, 15h, M2, Ensimag/INPG, France.
- Master : Claude Castelluccia, *Cyber Security*, 6h, M2, Laws School of University of Grenoble Alpes, France.
- Master : Claude Castelluccia, *Data Privacy*, 6h, M2, Laws School of University of Grenoble Alpes, France.
- Master : Claude Castelluccia, *Data Privacy*, 12h, SKEMA Business School, Sophia-Antipolis, France.
- Master : Daniel Le Métayer, *Privacy*, 12h, M2 MASH, Université Paris Dauphine, France.
- Master : Daniel Le Métayer, *Privacy*, 12h, M2, Insa Lyon, France.
- Master : Daniel Le Métayer, *Digital ethics*, 8h, M2, Insa Lyon, France.
- Master : Vincent Roca, *Wireless Communications*, 16h, M2, Polytech, University of Grenoble Alpes, France.
- Undergraduate course : Vincent Roca, *C Programming and Security*, 24h, L-Pro, IUT-2 (University of Grenoble Alpes), France.
- Undergraduate course : Vincent Roca, *Privacy in Smartphones and Internet of Things*, 3h, L-Pro, University of Grenoble Alpes, France.
- Master : Vincent Roca, *Privacy in Smartphones and Internet of Things*, 3h, M2, Ensimag/INPG, France.
- Master : Vincent Roca, *Privacy in Smartphones*, 3h, M2 (University of Cote-d'Azur), France.

10.1.5 E-learning

- MOOC: Cédric Lauradoux, Nataliia Bielova and Vincent Roca *"Protection de la vie privée dans le monde numérique"* on FUN-MOOC. From 2018 till May 2020, the MOOC has been open for 4 sessions and attracted in total **over 43,000 French-speaking participants** from all over the world. Since January 2021, the course is archived and can be freely accessed: `https://www.fun-mooc.fr/courses/course-v1:inria+41015+archiveouvert/about`.

10.1.6 Supervision

- PhD defended : Mathieu Thiery, *Objects connectés et vie privée : le long chemin restant* , December 2020, Vincent Roca and Arnaud Legout (DIANA team).
- PhD defended : Victor Morel, *Enhancing transparency and consent in the IoT*, September 2020, Daniel Le Métayer and Claude Castelluccia.
- PhD defended : Guillaume Celosia, *Privacy challenges in wireless communications of the Internet of Things* , September 2020, Mathieu Cunche and Daniel Le Métayer.
- PhD in progress : Supryia Adhatarao, *Privacy of E-learning systems* , start: March 2018, Cédric Lauradoux.
- PhD in progress : Coline Boniface, *Cyberweapons: from bug bounties to zero days* , start: March 2018, Cédric Lauradoux.
- PhD in progress : Raouf Kerkouche, *Privacy-Preserving Processing of Medical Data* , start: January 2018, Claude Castelluccia.
- PhD in progress : Clement Henin, *Explainable AI* , start: September 2018, Claude Castelluccia et Daniel Le Metayer.
- PhD in progress: Théo Jourdan, *Privacy-preserving machine learning in medical domain*, start: October 2018, Antoine Boutet.
- PhD in progress: Imane Fouad, *Detection of advanced Web tracking technologies*, start: January 2018, Nataliia Bielova and Arnaud Legout (DIANA team).
- PhD in progress: Michael Toth, *Dark patterns in GDPR consent*, start: December 2019, Nataliia Bielova and Vincent Roca.
- PhD in progress: Suzanne Lansade, *On pseudonymisation*, start: October 2020, Cédric Lauradoux and Vincent Roca.
- Intern (M2): Suzanne Lansade, *Pseudonymisation*, Cédric Lauradoux
- Intern (M2): Jan Aalmoe, *Analysis of geolocated advertising targeting*, Antoine Boutet
- Intern (L3): Hugo Degeorges, *IoT inference attack*, Antoine Boutet
- Intern (M1): Vasisht Duddu, *Privacy in Machine Learning*, Antoine Boutet
- Intern (M1): Guillaume Kessibi, *Personal data leaks on Android apps using dynamic analysis with FRIDA*, Vincent Roca and Mathieu Cunche
- Engineer: Adrien Baud, *Web platform for raising awareness of privacy issues*, Antoine Boutet
- Intern (M2): Remi Couderc, EPFL, *Dark Patterns*, Claude Castelluccia.

10.1.7 Juries

- Daniel Le Métayer : HDR Patricia Serrano Alvadaro (Nantes, 16/06/2020), PhD Thesis Joris Duguepéroux (Rennes, 1/10/2020).
- Nataliia Bielova: PhD Thesis Tobias Urban (Ruhr University Bochum, Germany, 03/07/2020).

10.2 Popularization

10.2.1 Interventions

- Vincent Roca: *"TousAntiCovid (TAC), ROBERT, DÉSIRÉ, où en est-on après 8 mois de travail ? Le point de vue PRIVATICS"*, 19/11/2021, Séminaire Inria Grenoble Rhône-Alpes, (Intranet news and link to the record).

10.2.2 Interviews by the media

- Nataliia Bielova: *"Données personnelles : les cookies résistent encore"*, 19/02/2020, MédiaPart, https://www.mediapart.fr/journal/france/190220/donnees-personnelles-les-cookies-resistent-encore.

- Antoine Boutet: *"L'app StopCovid : guérir le mal par la tech ?"*, 11/06/2020, actualité de l'INSA Lyon, https://www.insa-lyon.fr/fr/actualites/l-app-stopcovid-guerir-mal-par-tech .

11 Scientific production

11.1 Major publications

[1] A. Boutet and M. Cunche. 'Privacy Protection for Wi-Fi Location Positioning Systems'. In: *Journal of information security and applications* (Nov. 2020). URL: https://hal.inria.fr/hal-03045102.

[2] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Métayer and V. Roca. 'DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralized and decentralized systems'. working paper or preprint. May 2020. URL: https://hal.inria.fr/hal-02570382.

[3] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Métayer and V. Roca. 'ROBERT: ROBust and privacy-presERving proximity Tracing'. working paper or preprint. May 2020. URL: https://hal.inria.fr/hal-02611265.

[4] C. Castelluccia and D. Le Métayer Inria. 'Impact Analysis of Facial Recognition'. working paper or preprint. Feb. 2020. URL: https://hal.inria.fr/hal-02480647.

[5] G. Celosia and M. Cunche. 'Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols'. In: *Proceedings on Privacy Enhancing Technologies* 2020 (July 2020), pp. 26–46. DOI: 10.2478/popets-2020-0003. URL: https://hal.inria.fr/hal-02394619.

[6] I. Fouad, N. Bielova, A. Legout and N. Sarafijanovic-Djukic. 'Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels'. In: *PETS 2020 - 20th Privacy Enhancing Technologies Symposium*. PETs (Privacy Enhancing Technologies Symposium). Montréal, Canada, July 2020. URL: https://hal.inria.fr/hal-01943496.

[7] V. Roca and A. Begen. *Forward Error Correction (FEC) Framework Extension to Sliding Window Codes (RFC 8680)*. Ed. by R. E. (https://www.rfc-editor.org/). RFC 8680, Standards Track, TSVWG (Transport Area) working group of IETF (Internet Engineering Task Force), https://www.rfc-editor.org/rfc/rfc8680.html. Jan. 2020. URL: https://hal.inria.fr/hal-01345125.

[8] C. Santos, N. Bielova and C. Matte. 'Are cookie banners indeed compliant with the law?' In: *Technology and Regulation* 2020 (Dec. 2020), pp. 91–135. URL: https://hal.inria.fr/hal-02875447.

11.2 Publications of the year

International journals

[9] A. Boutet and M. Cunche. 'Privacy Protection for Wi-Fi Location Positioning Systems'. In: *Journal of information security and applications* (10th Nov. 2020). URL: https://hal.inria.fr/hal-03045102.

[10] G. Celosia and M. Cunche. 'Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols'. In: *Proceedings on Privacy Enhancing Technologies* 2020 (6th July 2020), pp. 26–46. DOI: 10.2478/popets-2020-0003. URL: https://hal.inria.fr/hal-02394619.

[11] M. Fiore, P. Katsikouli, E. Zavou, M. Cunche, F. Fessant, D. Le Hello, U. M. Aivodji, B. Olivier, T. Quertier and R. Stanica. 'Privacy in trajectory micro-data publishing: a survey'. In: *Transactions on Data Privacy* 13 (2020), pp. 91–149. URL: https://hal.inria.fr/hal-02968279.

[12] T. Jourdan, A. Boutet, A. Bahi and C. Frindel. 'Privacy-Preserving IoT framework for activity recognition in personal healthcare monitoring'. In: *ACM Transactions on Computing for Healthcare* (2nd Nov. 2020). URL: https://hal.inria.fr/hal-03045108.

[13] P. Laperdrix, N. Bielova, B. Baudry and G. Avoine. 'Browser Fingerprinting: A Survey'. In: *ACM Transactions on the Web* 14.2 (19th Apr. 2020), pp. 1–33. DOI: 10.1145/3386040. URL: https://hal.archives-ouvertes.fr/hal-02864872.

[14] C. Santos, N. Bielova and C. Matte. 'Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners'. In: *Technology and Regulation* 2020 (1st Dec. 2020), pp. 91–135. URL: https://hal.inria.fr/hal-02875447.

International peer-reviewed conferences

[15] G. Celosia and M. Cunche. 'Valkyrie: A Generic Framework for Verifying Privacy Provisions in Wireless Networks'. In: WiSec 2020 - 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. Linz, Austria, 8th July 2020. DOI: 10.1145/3395351.3399340. URL: https://hal.inria.fr/hal-02651398.

[16] N. Debs, T. Jourdan, A. Moukadem, A. Boutet and C. Frindel. 'Motion sensor data anonymization by time-frequency filtering'. In: 28th European Signal Processing Conference (EUSIPCO 2020). Amsterdam, Netherlands, 24th Aug. 2020. URL: https://hal.inria.fr/hal-02888083.

[17] V. Duddu, A. Boutet and V. Shejwalkar. 'Quantifying Privacy Leakage in Graph Embedding'. In: Mobiquitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. Cyberspace, United States, 7th Dec. 2020, pp. 1–11. URL: https://hal.inria.fr/hal-03013638.

[18] I. Fouad, N. Bielova, A. Legout and N. Sarafijanovic-Djukic. 'Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels'. In: PETS 2020 - 20th Privacy Enhancing Technologies Symposium. PETs (Privacy Enhancing Technologies Symposium). Montréal, Canada, 14th July 2020. URL: https://hal.inria.fr/hal-01943496.

[19] I. Fouad, C. Santos, F. Al Kassar, N. Bielova and S. Calzavara. 'On Compliance of Cookie Purposes with the Purpose Specification Principle'. In: IWPE 2020 - International Workshop on Privacy Engineering. Genova, Italy, 11th July 2020, pp. 1–8. URL: https://hal.inria.fr/hal-02567022.

[20] C. Henin and D. Le Métayer. 'Towards a framework for challenging ML-based decisions'. In: DeceptECAI 2020 - 1st International Workshop on Deceptive AI @ECAI2020. Santiago de Chili, Chile, 30th Aug. 2020, pp. 1–13. URL: https://hal.inria.fr/hal-02932467.

[21] C. Matte, N. Bielova and C. Santos. 'Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework'. In: 2020 IEEE Symposium on Security and Privacy (SP). San Francisco, United States, 18th May 2020, pp. 791–809. DOI: 10.1109/SP40000.2020.00076. URL: https://hal.inria.fr/hal-03117294.

[22] C. Matte, C. Santos and N. Bielova. 'Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?' In: APF 2020 - Annual Privacy Forum. Lisbon, Portugal, 1st Oct. 2020, pp. 1–24. URL: https://hal.inria.fr/hal-02566891.

National peer-reviewed Conferences

[23] A. Boutet, M. Cunche, S. Gambs, B. Nguyen and A. Laurent. 'DARC : Data Anonymization and Re-identification Challenge'. In: RESSI 2020 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Nouan-le-Fuzelier, France, 16th Dec. 2020. URL: https://hal.inria.fr/hal-02512677.

Conferences without proceedings

[24] L. Demir, M. Thiery, V. Roca, J.-M. Tenkes and J.-L. Roch. 'Optimizing dm-crypt for XTS-AES: Getting the Best of Atmel Cryptographic Co-Processors (long version)'. In: SECRYPT 2020 - 17th International Conference on Security and Cryptography. Paris, France: http://www.secrypt.icete.org/, 27th Apr. 2020, pp. 1–11. URL: https://hal.archives-ouvertes.fr/hal-02555457.

[25] C. Henin and D. Le Métayer. 'A Generic Framework for Black-box Explanations'. In: Pre-print of an article published in the International Workshop on Fair and Interpretable Learning Algorithms. Atlanta, United States, 10th Dec. 2020. URL: https://hal.inria.fr/hal-03127923.

Doctoral dissertations and habilitation theses

[26] G. Celosia. 'Privacy challenges in wireless communications of the Internet of Things'. Université de Lyon, 22nd Sept. 2020. URL: https://tel.archives-ouvertes.fr/tel-02974989.

[27] V. Morel. 'Enhancing Transparency and Consent in the Internet of Things'. Université de Lyon, 24th Sept. 2020. URL: https://hal.inria.fr/tel-02973666.

[28] M. Thiery. 'Connected devices and privacy: a long journey ahead'. Université Grenoble Alpes, 14th Dec. 2020. URL: https://hal.archives-ouvertes.fr/tel-03125022.

Reports & preprints

[29] L. T. Ancian and M. Cunche. *Re-identifying addresses in LoRaWAN networks*. Inria Rhône-Alpes; INSA de Lyon, 1st Sept. 2020. URL: https://hal.inria.fr/hal-02926894.

[30] N. Bielova, A. Boutet, C. Castelluccia, M. Cunche, C. Lauradoux, D. Le Métayer and V. Roca. *DESIRE: A Third Way for a European Exposure Notification System (SUMMARY - EN): Leveraging the best of centralized and decentralized systems*. Inria, 9th May 2020. URL: https://hal.inria.fr/hal-02570172.

[31] N. Bielova and C. Santos. *Feedback regarding EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Inria, 19th Oct. 2020. URL: https://hal.inria.fr/hal-03117323.

[32] N. Bielova and C. Santos. *Feedback to the Guidelines on the use of cookies and other tracking tools of the Italian Data Protection Authority*. Inria; Utrecht University, 17th Dec. 2020. URL: https://hal.inria.fr/hal-03079482.

[33] A. Boutet, N. Bielova, C. Castelluccia, M. Cunche, C. Lauradoux, D. Le Métayer and V. Roca. *Proximity Tracing Approaches - Comparative Impact Analysis*. INRIA Grenoble - Rhone-Alpes, 30th Apr. 2020. URL: https://hal.inria.fr/hal-02570676.

[34] A. Boutet, C. Castelluccia, M. Cunche, A. Dmitrienko, V. Iovino, M. Miettinen, T. D. Nguyen, V. Roca, A.-R. Sadeghi, S. Vaudenay, I. Visconti and M. Vuagnoux. *Contact Tracing by Giant Data Collectors: Opening Pandora's Box of Threats to Privacy, Sovereignty and National Security*. EPFL, Switzerland; Inria, France; JMU Würzburg, Germany; University of Salerno, Italy; base23, Geneva, Switzerland; Technical University of Darmstadt, Germany, 1st Dec. 2020. URL: https://hal.inria.fr/hal-03116024.

[35] C. Castelluccia. *From Dataveillance to Datapulation : The Dark Side of Targeted Persuasive Technologies*. 22nd July 2020. URL: https://hal.archives-ouvertes.fr/hal-02904926.

[36] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Métayer and V. Roca. *DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralized and decentralized systems*. 12th May 2020. URL: https://hal.inria.fr/hal-02570382.

[37] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Métayer and V. Roca. *ROBERT: ROBust and privacy-presERving proximity Tracing*. 18th May 2020. URL: https://hal.inria.fr/hal-02611265.

[38] C. Castelluccia and D. Le Métayer Inria. *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*. 17th Feb. 2020. URL: https://hal.inria.fr/hal-02480647.

[39] M. Cunche, A. Boutet, C. Castelluccia, C. Lauradoux and V. Roca. *On using Bluetooth-Low-Energy for contact tracing*. Inria Grenoble Rhône-Alpes; INSA de Lyon, 23rd June 2020. URL: https://hal.inria.fr/hal-02878346.

[40] M. Cunche and A. Ratel. *IoT & Privacy - Comment assurer la confidentialité sur les réseaux sans fil ? L'exemple du BLE*. INSA Lyon; SPIE ICS, 20th Jan. 2020. URL: https://hal.inria.fr/hal-03020342.

[41] V. Duddu, A. Boutet and V. Shejwalkar. *GECKO: Reconciling Privacy, Accuracy and Efficiency in Embedded Deep Learning*. 5th Oct. 2020. URL: https://hal.inria.fr/hal-02958323.

[42] C. Henin and D. Le Métayer. *A Multi-layered Approach for Interactive Black-box Explanations*. Inria - Research Centre Grenoble – Rhône-Alpes; Ecole des Ponts ParisTech, 4th Mar. 2020. URL: https://hal.inria.fr/hal-02498418.

[43] R. Kerkouche, G. Ács and C. Castelluccia. *Federated Learning in Adversarial Settings*. 27th Oct. 2020. URL: https://hal.archives-ouvertes.fr/hal-02968257.

[44] G. Kessibi, M. Cunche, A. Boutet, C. Castelluccia, C. Lauradoux and V. Roca. *Analysis of Diagnosis Key distribution mechanism in contact tracing applications based on Google-Apple Exposure Notification (GAEN) framework*. 13th July 2020. URL: https://hal.inria.fr/hal-02899412.

[45] R. C. Ngueveu, A. Boutet, C. Frindel, S. Gambs, T. Jourdan and C. Rosin. *DYSAN: Dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks*. inria, 21st Feb. 2020, p. 27. URL: https://hal.inria.fr/hal-02512640.

[46] V. Roca, N. Bielova, A. Boutet, C. Castelluccia, M. Cunche, C. Lauradoux and D. Le Métayer. *DESIRE : une Troisième Voie pour un Système Européen de Notification d'Exposition: Tirer le meilleur des systèmes centralisés et décentralisés (RESUME - FR)*. Inria, 9th May 2020. URL: https://hal.inria.fr/hal-02568730.

[47] M. Toth, N. Bielova, C. Santos, V. Roca and C. Matte. *Contribution to the public consultation on the CNIL's draft recommendation on "cookies and other trackers"*. 25th Feb. 2020. URL: https://hal.inria.fr/hal-02490531.

Other scientific publications

[48] G. Celosia and M. Cunche. *DEMO: Venom: a Visual and Experimental Bluetooth Low Energy Tracking System*. Linz, Austria, 8th July 2020. DOI: 10.1145/3395351.3401696. URL: https://hal.inria.fr/hal-02651359.

[49] V. Roca. *From ROBERT to DESIRE exposure notification: situation and lessons learned*. Vienna, Austria, 11th Sept. 2020. URL: https://hal.inria.fr/hal-02936838.

[50] V. Roca and A. Begen. *Forward Error Correction (FEC) Framework Extension to Sliding Window Codes (RFC 8680)*. 15th Jan. 2020. URL: https://hal.inria.fr/hal-01345125.

[51] V. Roca and B. Teibi. *Sliding Window Random Linear Code (RLC) Forward Erasure Correction (FEC) Schemes for FECFRAME (RFC 8681)*. 15th Jan. 2020. URL: https://hal.inria.fr/hal-01630089.

[52] M. Saito, M. Matsumoto, V. Roca and E. Baccelli. *TinyMT32 Pseudorandom Number Generator (PRNG) (RFC 8682)*. 15th Jan. 2020. URL: https://hal.inria.fr/hal-02449210.